* NOTICES *

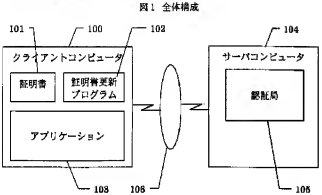
JPO and INPIT are not responsible for any
damages caused by the use of this translation.

1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

DRAWINGS

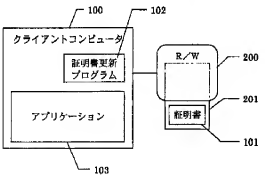
[Drawing 1]

図1 全体構成



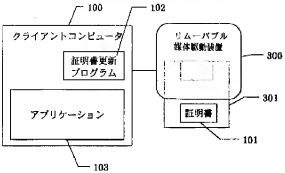
[Drawing 2]

図2 証明書格納先がＩＣカードの場合



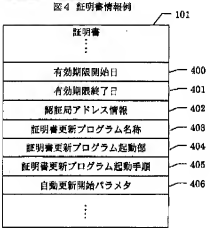
[Drawing 3]

図3 証明書格納先がリムーバブル媒体の場合



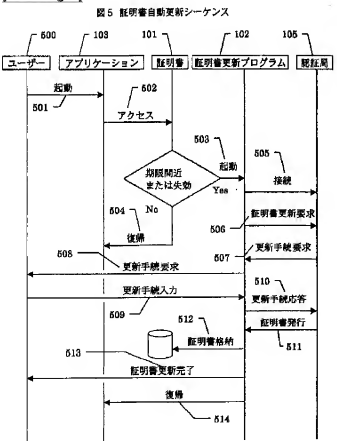
[Drawing 4]

図4 証明書情報例



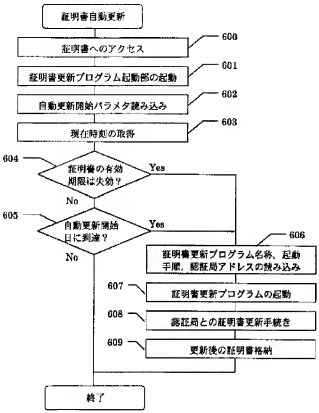
[Drawing 5]

図5 証明書自動更新シーケンス



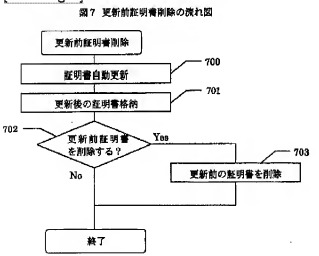
[Drawing 6]

図6 証明書自動更新の流れ図



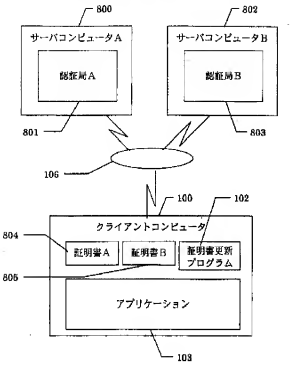
[Drawing 7]

図7 更新前証明書削除の流れ図



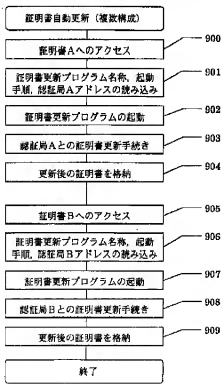
[Drawing 8]

図8 認証局と証明書が複数の構成の場合



[Drawing 9]

図9 認証局と証明書が複数の場合の証明書自動更新の流れ図



[Translation done.]

* NOTICES *

JPO and INPIT are not responsible for any
damages caused by the use of this translation.

1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

DESCRIPTION OF DRAWINGS

[Brief Description of the Drawings]
[Drawing 1]In order to explain this invention, it is an entire configuration figure of **.
[Drawing 2]It is a figure showing the example of composition of a client.
[Drawing 3]It is a figure showing the example of composition of a client.
[Drawing 4]It is a figure showing an example of the information recorded on a certificate.
[Drawing 5]It is a figure showing an example of the overall sequence in certificate automatic-updating processing.
[Drawing 6]It is a flow chart of certificate automatic-updating processing.
[Drawing 7]It is a flow chart when deleting the certificate before updating.
[Drawing 8]It is an entire configuration figure in case there are two or more certificate authorities.
[Drawing 9]It is a flow chart of the certificate automatic-updating processing in certificate automatic-updating processing.
[Description of Notations]
100 Client computer
101 Certificate
102 Renewal program of a certificate
103 Application
104,800,802 Server computer
105 Certificate authority
200 IC card reader writers
201 IC card
300 Removable medium drive
301 Removable medium
801 Certificate authority A
803 Certificate authority B
804 Certificate A
805 Certificate B

* NOTICES *

JPO and INPIT are not responsible for any
damages caused by the use of this translation.

1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

DETAILED DESCRIPTION

[Detailed Description of the Invention]
[0001]
[Field of the Invention]This invention relates to the certificate automatic-updating device and updating method which can update automatically the public key certification published by the certificate authority.
[0002]
[Description of the Prior Art]Internet technique spreads quickly and follows on this in recent years -- tapping of the data on the Internet or intranet -- altering and becoming completely -- etc. -- the problem of security has occurred. In order to solve such a problem, the security art which uses a public-key crypto system generally came to be adopted now. A public-key crypto system uses the key of the couple which consists of a secret key and a public key, and said secret key is kept in secrecy so that it may not leak to others. On the other hand, a public key is opened to others and used for the cryptogram creation to self, etc. For this reason, the relation between said public key and its owner must be guaranteed by the 3rd person. It is carried out when the certificate authority which is usually said 3rd person organization publishes a public key certification, and this guarantee is ****.
[0003]
[Problem(s) to be Solved by the Invention]The user who uses said certificate in said conventional technology, When [to which the term of validity of the certificate published from the certificate authority became close] invalidated [case or], the homepage of a certificate authority must be accessed via a web browser, and the renewal registration work of a certificate must be done according to the update procedure of the certificate in the certificate authority. That is, since updating operation of said certificate was performed via the help, the updating failure of a certificate, the update procedure failure, etc. had produced it frequently.
[0004]In the application which performs user authentication, encryption, decryption, signature, assay, etc., When the term of validity of a certificate is close, display a message to that effect and the updating operation of a subsequent certificate is demanded from a user, In the case of expiration, there are some which display an error message, restrict the function which stops application or needs a certificate, and start application. In this case, in order to update a certificate, it is required to once stop application and to reboot.
[0005]It is in this invention providing the certificate automatic-updating device which can update a certificate automatically, when [which was made in view of said problem, gave information required for the updating

operation of a certificate to the certificate itself, and became term-of-validity nearness] invalidated [case or].
[0006]
[Means for Solving the Problem]The following means were used for this invention in order to solve the above-mentioned technical problem.
[0007]Memory storage which stores a renewal program of a certificate which connects with a server computer which has a certificate authority function, and updates a certificate automatically, and said certificate, It consists of a client computer which is provided with an application program using said certificate, connects with said server computer after the last stage of the term of validity of said certificate, or an end of the term of validity, and requires automatic renewal of said certificate of said server computer, Said certificate is provided with a renewal program starting part of a certificate which starts expiration date information and said renewal program of a certificate, While connecting with said server computer after the last stage of the term of validity of said certificate, or an end of the term of validity and requiring automatic renewal of said certificate of said server computer, an updated certificate is received and it stores in said memory storage.
[0008]
[Embodiment of the Invention]Drawing 1 thru/or drawing 5 are used for below, and the embodiment of this invention is described to it. Drawing 1 is an entire configuration figure for explaining this invention. In a figure, 100 is a client computer which the user who uses a certificate holds. 101 is the certificate stored in memory storage, such as a hard disk of the client computer 100. 102 is a renewal program of a certificate for connecting with a certificate authority and actually updating a certificate. 103 is application which uses security art, such as encryption and signature grant, using the certificate 101. As long as this application is application which uses the certificate 101, it may be what kind of application also in the business oriented application which the web browser or the user developed uniquely. 104 is the server computer provided with the certificate authority function to publish the certificate 101. 105 is the certificate authority built on the server computer 104. 106 is a wide area network which has connected the client computer 100 and the server computer 104.
[0009]Drawing 2 is an example of composition of a client in case the storage location of the certificate 101 is an IC card. 200 is the IC card reader writers linked to the client computer 100 for writing the information in an IC card. 201 is the IC card which stored the certificate 101. According to this invention, not only the certificate 101 stored in the hard disk but automatic renewal of the certificate 101 stored in IC card 201 can be performed.
[0010]Drawing 3 is an example of composition of a client in case the storage location of the certificate 101 is a removable medium. 300 is a removable medium drive connected to the client computer 100 for writing the information on the removable intermediation inside of the body. 301 is the removable medium which stored the certificate 101. As the removable medium 301, a floppy (registered trademark) disk, a magneto-optical disc, etc. are raised, for example. According to this invention, not only the certificate 101 stored in the hard disk but automatic renewal of the certificate 101 stored in the removable medium 301 can be performed.
[0011]Drawing 4 is an example of the information recorded on the certificate 101 by said certificate authority. 400 is a term-of-validity opening day of the certificate 101. 401 is an end date of the term of validity of the certificate 101. 402 is certificate authority address information. This certificate authority address information 402 can be made into URL or an IP address depending on the connection specification to the certificate

authority 105. It connects with the certificate authority 105 with reference to the certificate authority address information 402, and 403 is a renewal program name of a certificate for updating the certificate 101, for example, specifies the renewal program 102 of a certificate. 404 is a renewal program starting part of a certificate for actually starting said renewal program 102 of a certificate. When access is performed from the application 103 to the certificate 101, this renewal program starting part of a certificate operates first. 405 is the renewal program activation procedure of a certificate which showed the procedure of starting said renewal program 102 of a certificate. It is the automatic-updating start parameter which specified whether 406 would be made to update a certificate automatically from what day [of the end date 401 of the term of validity] before.

[0012]Drawing 5 shows an example of the overall sequence in a certificate automatic-updating device. The user 500 does application 103 starting 501. If the application 103 starts, it will be used as the certificate 101 which is needed for performing encryption, a signature, etc. access 502. The storage location of the certificate 101 is either of the removable media 301, such as a hard disk in the client computer 100, IC card 201, or a floppy disk.

[0013]or [that current time's end date 401 of the term of validity of said certificate 101 is close] -- or when invalidated, the renewal program 102 of a certificate shown with the renewal program name 403 of a certificate according to the renewal program activation procedure 405 of a certificate stored in the certificate is carried out starting 503. On the other hand, when the end date 401 of the term of validity of the certificate 101 is not the nearness of current time and it is not invalidated, it controls return 504 to the application 103 as it is.

[0014]If the renewal program 102 of a certificate is started, according to the certificate authority address information 402 of the certificate 101, it will take connection 505 for the certificate authority 105 via a network. Then, the renewal program 102 of a certificate performs the certificate update request 506 to the certificate authority 105. The certificate authority 105 publishes the updating procedure demand 507 to the renewal program 102 of a certificate, in order to acquire information actually required for renewal of a certificate, if the renewal request 506 of a certificate is received. The renewal program 102 of a certificate which received the updating procedure demand 507 publishes the updating procedure demand 508, in order to acquire information required for renewal of a certificate from a user to the user 500.

[0015]The user 500 who received the updating procedure demand 508 does information required for renewal of a certificate input 509. The renewal program 102 of a certificate returns the updating procedure response 510 to the certificate authority 105 based on said information carried out input 509. The certificate authority 105 which received the updating procedure response 510 performs certificate issuing 511 to the renewal program 102 of a certificate according to the updating procedure response 510. The renewal program 102 of a certificate which received the certificate after updating receives any of the removable media 301, such as a hard disk or IC card 201, and a floppy disk, they are, and performs certificate storing 512. Then, the renewal program 102 of a certificate notifies the completion 513 of renewal of a certificate which shows that the updating procedure of the certificate was successful to the user 500, and controls return 514 to the application 103. Thereby, since it connects automatically and a certificate is updated even if the user 300 is not conscious of connection with the certificate authority 105, the user can continue the application 103 which performs business etc., without paying attention on the end date 401 of the term of validity of the certificate 101.

[0016]Drawing 6 shows the flow chart of certificate automatic-updating processing. It is already assumed that

the application 103 is started. First, in Step 600, access to a certificate from the application 103 is performed. In Step 601, the renewal program starting part 404 of a certificate stored in the certificate 101 is started. In Step 602, the renewal program starting part 204 of a certificate acquires current time in automatic-updating start parameter reading and Step 603.

[0017]In Step 604, the acquired current time is compared with the end date 401 of the term of validity stored in the certificate 101, when the term of validity of a certificate is invalidated, it progresses to Step 606, and when not invalidated, it progresses to Step 605. In Step 605, a part for the days specified with the automatic-updating start parameter 406 is subtracted from the end date 401 of the term of validity, and it asks for an automatic-updating beginning date, and compares with this date and current time. When having reached the automatic-updating beginning date, it progresses to Step 606, and processing is ended when that is not right. In Step 606, reading of the renewal program name of a certificate, an activation procedure, and a certificate authority address is performed. In Step 607, the renewal program starting part 204 of a certificate starts the renewal program of a certificate based on said read information. Renewal procedure of a certificate is performed through the sequence which connected the started renewal program 102 of a certificate with the certificate authority 105 via the network, for example, was shown by the sequence of drawing 5. In Step 609, if the certificate after updating is published from the certificate authority 105, the certificate after renewal of this will be received, it will store in a recording medium, and processing will be ended. A storage location can be used as the recording medium with which the certificate before updating was stored.

[0018]Drawing 7 shows a flow chart when deleting the old certificate before updating, after updating a certificate automatically. Here, already let the certificate 101 be term-of-validity nearness or the conditions to which it is invalidated and automatic updating is carried out. First, in Step 700, certificate automatic updating explained in full detail by drawing 5 and drawing 6 is performed, and the certificate which received and received the certificate after updating from the certificate authority 105 is stored in Step 701. In Step 702, a dialog message is displayed and it asks a user whether delete the certificate before updating. When the reply of the purport that a user deletes is inputted, it progresses to Step 703, and processing is ended when that is not right. The certificate before updating is deleted in Step 703. Thereby, the memory consumption of the storage by an old certificate can be eliminated.

[0019]Two or more certificate authorities exist and drawing 8 shows an entire configuration figure in case that each of a certificate authority certificate [from] is published. 800 is the server computer A. 801 is the certificate authority A built on the server computer A800. 802 is the server computer B. 803 is the certificate authority B built on the server computer B802. 804 is the certificate published from the certificate authority A801 stored in the hard disk of the client computer 100. 805 is the certificate similarly published from the certificate authority B803. When there are two or more certificate authorities, the certificate after updating can be received from each certificate authority in the same procedure as the case of the singular number mentioned above.

[0020]Drawing 9 shows the flow chart of the certificate automatic-updating processing in the composition shown by drawing 8. Here, are invalidated and already let the certificate A804 and the certificate B805 be term-of-validity nearness or the conditions to which automatic updating is carried out. First, in Step 900, access to the certificate A is performed from the application 103. In Step 901, the renewal program starting part 404 of

a certificate reads the address of the renewal program name of a certificate, an activation procedure, and the certificate authority A. In Step 902, the renewal program of a certificate is started based on the read information. In Step 903, the started renewal program 102 of a certificate performs renewal procedure of a certificate with the certificate authority A. In Step 904, if the certificate after updating is published from the certificate authority A801, the certificate after updating is received and stored.

[0021]In Step 905, access to the certificate B is performed from the application 103. In Step 906, the renewal program starting part 404 of a certificate reads the address of the renewal program name of a certificate, an activation procedure, and the certificate authority B. In Step 907, the renewal program of a certificate is started based on the read information. In Step 908, the started renewal program 102 of a certificate performs renewal procedure of a certificate with the certificate authority B. In Step 909, if the certificate after updating is published from the certificate authority B801, the certificate after updating is received and stored.

[0022]By the above, automatic renewal of two or more certificates A804 and the certificate B805 which were published from two or more certificate authorities A801 and certificate authorities B803 is completed. Thereby, also in the composition which uses again the certificate [each] published from the certificate authority by plurality, automatic renewal of a certificate of a certificate authority is attained.

[0023]As explained above, when [which gave information required for the updating operation of a certificate to the certificate itself, and became term-of-validity nearness] invalidated [case or], it connects with a certificate authority automatically and a certificate is updated. Therefore, the user who performs business using the application which secures security using said certificate, Even if not conscious of connection with the certificate authority which is the term of validity and the certificate issuing organ of a certificate, When invalidated and application accesses [the term-of-validity nearness of a certificate, or] a certificate, it can connect with a certificate authority automatically, a certificate can be updated, and control can be returned to application as it is. For this reason, the time and effort which investigates an address, URL, etc. of troublesomeness, such as a stop of application and a reboot, and the certificate authority for having a certificate published is reduced, and the user can prevent suspension of the business by updating failure of a certificate, etc. The above-mentioned automatic updating can be mounted without adding especially a hand to any applications which can use a certificate. For this reason, it becomes easy to aim at thoroughness of renewal of a certificate to a user.

[0024]

[Effect of the Invention]As explained above, according to this invention, when [which gave information required for the updating operation of a certificate to the certificate itself, and became term-of-validity nearness] invalidated [case or], the certificate automatic-updating device which can update a certificate automatically can be provided.

[Translation done.]

* NOTICES *

JPO and INPIT are not responsible for any
damages caused by the use of this translation.

1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

CLAIMS

[Claim(s)]
[Claim 1]A certificate automatic-updating device comprising:
Memory storage which stores a renewal program of a certificate which connects with a server computer which has a certificate authority function, and updates a certificate automatically, and said certificate.
It consists of a client computer which is provided with an application program using said certificate, connects with said server computer after the last stage of the term of validity of said certificate, or an end of the term of validity, and requires automatic renewal of said certificate of said server computer, A renewal program starting part of a certificate in which said certificate starts expiration date information and said renewal program of a certificate.

[Claim 2]A certificate automatic-updating device, wherein said client computer is provided with a removable medium drive which stores said certificate information in a removable medium in a statement of claim 1.
[Claim 3]Memory storage which stores a renewal program of a certificate which connects with a server computer which has a certificate authority function characterized by comprising the following, and updates a certificate automatically, and said certificate, A certificate automatic-updating method which consists of a client computer which is provided with an application program using said certificate, connects with said server computer after the last stage of the term of validity of said certificate, or an end of the term of validity, and requires automatic renewal of said certificate of said server computer.
A step which connects said certificate automatic-updating method to said server computer after the last stage of the term of validity of said certificate, or an end of the term of validity, and requires automatic renewal of said certificate of said server computer.
A step which starts said renewal program of a certificate.
A step linked to a server computer.
A step which receives issue of a certificate from a server computer, and a step which accumulates a certificate which won popularity in memory storage.

[Claim 4]A recording medium characterized by comprising the following which recorded a program and in which computer reading is possible.

A step which connects with a server computer which has an authentication function, and requires automatic renewal of said certificate of this server computer after the last stage of the term of validity of a certificate stored in a client computer, or an end of the term of validity.
A step which starts a renewal program of a certificate stored in a client computer based on this demand.
A step which connects a client computer to a server computer.
A step which receives issue of a certificate from a server computer, and a step which accumulates a certificate which won popularity in memory storage.

[Claim 5]It has a server characterized by comprising the following which publishes a certificate, While connecting said client computer to said server computer after the last stage of the term of validity of said certificate, or an end of the term of validity and requiring automatic renewal of said certificate of said server computer, A certificate automatic update system receiving an updated certificate and storing in said memory storage.
Memory storage which stores a renewal program of a certificate which connects with a server computer which has a certificate authority function, and updates a certificate automatically, and said certificate.
It has an application program and a certificate authority function to use said certificate, and is the address information of a certificate authority at least.

[Translation done.]